AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

AT&T Cingular Flex EA211101 Cell Phone, More Fully Described in Attachment A and Currently Located at Binghamton FBI, 15 Henry Street, #321, Binghamton, NY

Case No. 3:23-MJ-243 (ATB)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

AT&T Cingular Flex EA211101 Cell Phone, More Fully Described in Attachment A and Currently Located at Binghamton FBI, 15 Henry Street, #321, Binghamton, NY

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

AT&T Cingular Flex EA211101 Cell Phone, More Fully Described in Attachment A and Currently Located at Binghamton FBI, 15 Henry Street, #321, Binghamton, NY

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Sections 2252A(a)(2)(A), (a)(5)(B); 2422(b); 2251(a); 2250(a); & 1470	Receipt and Possession of Child Pornography; Attempted Enticement of a Minor; Sexual Exploitation of a Minor; Failure to Register an E-Mail Address as Required by SORNA; and Transferring Obscene Material to a Minor

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jenelle Corrine Bringuel, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 04/27/2023

Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jenelle Corrine Bringuel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in 18 U.S.C. § 2516. As such, I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510(7).

2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, online enticement of minors, and child pornography. I have gained experience through training by the FBI and the investigations in which I have personally participated. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I am currently investigating Joseph Green who I suspect has knowingly received and possessed child pornography, sexually exploited children, failed to register an e-mail address as required by SORNA, transferred obscene material to a minor, and attempted to entice a minor, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) & (a)(5)(B), 2251(a), 2250(a), 1470 and 2422(b) ("Subject Offenses").

4. This affidavit is submitted in support of a warrant to search (1) AT&T Calypso Model U318AA cell phone; IMEI 86422605037953 – Blue in color, and (2) AT&T Cingular Flex EA211101 cell phone; IMEI 353786872430704 (collectively, "**Subject Electronic Devices**") that the United States Probation Office for the Northern District of New York ("Probation Office") seized from Green. The **Subject Electronic Devices** were seized from Green on December 7,

2021, and March 27, 2023, respectively, as he was not permitted to possess the devices based on the terms of his probation. The **Subject Electronic Devices** are currently located at the FBI Binghamton Resident Agency, 15 Henry Street #321, Binghamton, NY.

5. The statements and facts set forth in this affidavit are based in significant part on my review of written documents obtained from the United States Probation Office (USPO), conversations with probation officers, and my personal training and experience. Since this affidavit is being submitted for the limited purposes of a securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses are presently located on the **Subject Electronic Devices**.

FACTS SUPPORTING PROBABLE CAUSE

6. On April 19, 2012, Green was sentenced in the United States District Court for the Northern District of New York to 60 months imprisonment and a 15 year term of supervised release after pleading guilty to distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2).

7. On October 10, 2016, Green began his term of supervised release. On December 7, 2021, Green submitted to a maintenance polygraph examination by the USPO and failed the exam. Green was not truthful when asked about possessing an internet capable device. The polygrapher was able to "clear" Green and Green admitted to purchasing an internet-capable "smart phone" two days prior on December 5, 2021. Green had multiple opportunities to disclose this to this officer and the polygrapher and choose not to prior to the exam. Green did later admit that he thought he could pass the exam and he made a poor decision. This phone (**Subject Electronic Device** #1) was taken into custody by the USPO. In addition to Green possessing an internet-

capable device, he also created a new email address. On December 6, 2021, he created greenjXXXX@gmail.com in order to use the newly acquired smart phone. This also was not disclosed prior to the polygraph. After being caught by the USPO, Green as required by law, registered the new email address with the Binghamton Police Department and the New York State Sex Offender Registry within 10 days. Green's probation officer had lengthy discussions with Green regarding the above-mentioned conduct and his conditions of release were reviewed to ensure there was no further non-compliance or misunderstandings. As punishment for his non-compliance with his release conditions Green received 50 hours of community service.

8. On March 27, 2023, USP Officer Jeff Clinton met with Green at his residence for a home contact. During the home contact, the probation officer requested permission to review Green's phone. Green provided the probation officer verbal consent to review his phone. Green provided probation with a gray in color, AT&T flip phone (**Subject Electronic Device #2**). The probation officer discovered what appeared to be adult nude images on the device. Green reported he had been sent the images by another party. The probation officer discovered a hidden application, "Randomly Chat". Green initially denied using the application. The probation officer checked Green's text messages and found sexual text messages between Green and individuals who informed Green in the messages that they were under the age of eighteen. When further questioned, Green admitted that he met these individuals on the Randomly Chat application. He further stated he has communicated with at least five females, under the age of eighteen, with the youngest being 12 years of age. Green stated that he communicated with the minors between February 2023 to the present. Green stated that on a few occasions he has received photos that appeared to be nude minors, however, he stated he immediately deleted the photos. At that time the probation officer seized Green's cellular telephone. On March 28, 2023, USPO Scott Shanahan

used Cellebrite[1] to attempt to examine the telephone that was seized from Green. The search returned minimal results. USPO Clinton manually searched the phone and discovered two videos that show a male subject masturbating. One of the videos shows the male subject masturbating to ejaculation. The probation office also reviewed the contents of the text messages which revealed sexual conversations between Green and individuals who reported their ages to be 12 and 15. Some of those conversations according to the USPO's report include the following:

> On March 22 and 23, 2023, Green corresponds via text message with an individual who tells him she is 12 years old.
>
> Green: And I like ur age girls
> 12: Mhm
> Green: Never met a man that gets turned on by lil girls
> 12: Usually see them on tv lol
> Green: Lol true going to court
> Green: Lol I want to have sex with u
> The 12 year old tells Green that she got in trouble at school and grounded at home. She tells Green about her mom punishing her.
> Green: O sorry u got me thou
> Green: Ur fav perv
> Green later tells the child he is watching the television show Dance Moms.
> 12: Never heard of it
> Green: Its about young girls dance
> Green: Class
> Green: Thex were leotards
> Green: And I masterbate to thdn
> Green: lol
> Green: I cant help it lol they get me hard
> 12: I wish is was at my gramma house I love your cock mmm
> Green: Lol
> Green: I love ur lil tits and ur bald pussy
> Green: I love u to
> Green: I got a 12 yr old friend lol
> Green: whth benefits
> 12: I wanna be more than friends
> Green: Gf
> 12: Mhm

[1] Cellebrite is a software package used by law enforcement for the purpose of extracting the contents to cellular telephones.

Green: Ok ur my gf
12: Yay
Green: I wanna lick u
Green: I wanna have sex wit u lol
Green: I wanna cum in ur pussy
Green: Fubk the law
Green: It should be leagle for to fuck u

On March 25 and 26, 2023, Green corresponds via text message with an individual who tells him she is 15 years old.

Green: Last time we talk I think we had fun lol
15: Yea
Green: Ur a grea young lady
15: And you're a great man
Green: I would love to see u for real
15: Me too
Green: I wanna explore that bald pussy while I am down there
Green: U be the first I tastf at ur age
Green: Well no to many men like wat I like lol
Green attempts to get the child to send him photos and talk on the phone. The child tells him her family is home, so it is not a good time to talk. She states "Yah, I wish I was 18 then it wouldnt be weird to be with you."
Green: True
Green: How long I got wait till ur 18
15: I turn 16 in june
Green: And it will be great no one judgeing me for my choice of who I fall in love with
Green: I am glad we met in a stranger chat and hit it off
The two engage in role play where the child is a student and Green is her teacher.
Green: I run my hadn down ur thigh raising ur leg and slide penis in u
Green: I change my place no I am behind u thrusting into
Green: And u look back at me
Green: Where do u want me to finish in u or us want me to pull out
Green: Ur the girl I want to be with
15: And ur the guy I want to be with
The two discuss the child's school and Green begin to again role play
Green: Ur a a student
15: Mmmm
Green: As I fck that tight virgin pussy
Green: I like the feel of a smooth girl
15: I start sucking faster
Green: I start to fuck ur mouth until I cum in ur mouth
Green: I am the naughty nabor who like young girls
Green: And u live next door to me
Green: O baby I stick in ur ass and reach around and finger u as I hit that ass
15: Moaning loudly at the same time

Green: I love to fuck that ass
15: I know you do
Green: I start to cum in ur ass
When I turn 18 we can just fuck anyway anytime anywhere
Green: Legal or not i still fuck u
15: I would fuck you now if I could
Green: So true me to
Green: We are both in control to say yes or no and u no wat consent is as do i

9. On March 30, 2023, Green reported to the probation office. He admitted that he met the minors, with whom he was conversing, using the "Randomly Chat" application on his phone. He stated that he started to using the application to correspond with adults, but then began targeting minors. Green admitted to engaging in sexual conversations with six or seven children. Green further admitted to sending nude photos of himself and videos of himself masturbating, to three or four children. Green stated he knew the recipients were under the age of eighteen when he sent the photos and videos. Green additionally admitted to conversing with a 16-year-old in text messages and through a voice call. Green reported the 16- year-old lived in a group home in Tennessee. Green reported the 16-year-old called him after they had exchanged sexual text messages, and she masturbated while Green listened on the phone and encouraged the minor's sexual conduct.

10. An arrest warrant based on a Supervisory Release Petition was issued for Green by the Honorable Judge Thomas J. McAvoy on April 12, 2023, and Green is currently in custody pending his final revocation hearing.

COMPUTERS AND CHILD PORNOGRAPHY

11. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experiences and training of other law enforcement officers with whom I have had discussions, I know that computers, including desktop computers, laptops, SD cards, cellular telephones, and other electronic media, basically serve four functions in

connection with child pornography: production, communication, distribution, and storage.

12. A computer's ability to store images in digital form makes such devices an ideal repository for child pornography. The size of the electronic storage media used in computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. SD cards can also be used to copy, store, transport and transmit digital images.

13. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

14. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Gmail, among others. The online services allow a user to set up an account with a remote computing device that provides e-mail services as well as electronic storage of computer files with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

15. As with most digital technology, communications made from a computer are often saved or stored on that device. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer' web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-

peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a computer can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

16. I know that data files, including digitized images, correspondence, records, communications, and other matters sought by this Warrant, can be stored in a variety of digital formats on a computer using various software applications. For example, digital still images are commonly created and stored as JPEG files and identified by .jpg or .jpeg in filename suffix. Digital still images may also be created, converted, or stored, among other things as an Adobe Acrobat file (using the suffix .pdf); embedded within a word processing document (using the suffix.wpd or .doc); or converted to another graphics file format (.gif or .tif). In addition, data filenames typically include a suffix associated with the application that created or modified the file (e.g., XXX.pdf indicates a file associated with Adobe Acrobat). A file name, however, can be manipulated to include a suffix that conceals its true format, or is not readily recognized by or associated with any software application. Accordingly, because digitized versions of items sought by this Warrant can be created and/or stored in any number of digital file formats, it is necessary to search every data file stored on a computer or other data storage device to locate and seize such items.

17. Mobile communication devices are commonly used for both personal and business use. These devices range from simple mobile telephones to complex devices encompassing numerous technologies in one hand-held device. They are electronically powered and typically combine the ability to store and transfer data along with serving as a communications facility.

Mobile communication devices are essentially ultra-small computers, and in my experience, they are often a medium on which child pornography is stored. Mobile communication devices often include an SD card and users can sometimes select to have data on their mobile communication devices saved directly to an SD card.

18. Based on my training and experience, I know that mobile communication devices can be used to transmit both written messages (e.g., text messages) as well as images. Cellular telephones, for example, have the capacity to store voice mail messages, names, telephone numbers, addresses, sent and received text messages, and images in their internal memory. Many cellular telephones have the capability to capture digital photographic images and videos, store them in internal memory or on SD cards, and transmit them to one or more different cellular telephones. I also know that individuals sometimes use cellular telephones to produce, send, and receive child pornographic images.

COLLECTORS OF CHILD PORNOGRAPHY

19. Individuals who are interested in child pornography may want to keep the child pornography files they create or receive for additional viewing in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy of their homes, on computers, on external hard drives, on cellular telephones, or in other secure locations. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished fantasies, the collector rarely, if ever, disposes of his collection. The collection may be culled and refined, but, over time, the size of the collection tends to increase. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them over time.

20. Individuals who collect child pornography may search for and seek out other like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, instant messaging, and other vehicles.

21. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

22. Individuals who collect child pornography may keep names, electronic mail addresses, cellular and telephone numbers, or lists of persons who have shared, advertised, or otherwise made known their interest in child pornography or sexual activity with minor children. These contacts may be maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

23. I am trained in computer and cellular telephone evidence recovery and have extensive knowledge about the operation of cellular telephones and computer systems, including the correct procedures for the seizure and analysis of these systems.

24. Based on my knowledge, training, and experience, I am aware that electronic files

or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered months or years later using specialized forensic tools. This is so because when a person "deletes" a file on a computer or cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

25. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data or process in a "swap" or "recovery" file. Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache" located on the computer. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

26. Apart from user-generated files, an electronic device may contain electronic evidence of when it was used, what it was used for, and more importantly, who used it recently and in the past. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence or physical location. For example, registry information, configuration files, user profiles, e-mail address books, "chats," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of who used or controlled the computer or storage medium at a relevant time in question.

SEARCH METHODOLOGY TO BE EMPLOYED

27. Searches and seizures of evidence from a computer or cellular telephone commonly requires agents to download or copy information from those devices and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computers and cellular telephones can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computers and cellular telephones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and application, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or

normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. The search procedure for the **Subject Electronic Devices** may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data on the **Subject Electronic Devices** to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents and scanning storage areas;

e. performing key word searches to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

29. Because the **Subject Electronic Devices** are already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises.

Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. Based upon the above information, there is probable cause to believe that evidence of violations of violations of 18 U.S.C. §§ 2252A(a)(2)(A) & (a)(5)(B) (Receipt and Possession of Child Pornography), 2422(b) (attempted enticement of a minor), 2251(a)(sexual exploitation of a minor), 2250(a) (failure to register an e-mail address as required by SORNA), and 1470 (transferring obscene material to a minor) as outlined in Attachment B of this Affidavit, will be found within the **Subject Electronic Devices**. Therefore, based upon the information contained in this affidavit, I request that this Court issue the attached search warrant authorizing the search of the contents of the **Subject Electronic Devices**, set forth in Attachment A, for the items more particularly described in Attachment B.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Jenelle Corrine Bringuel
Special Agent
Federal Bureau of Investigation

I, the Honorable Andrew T. Baxter, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on April 27, 2023, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

HONORABLE ANDREW T. BAXTER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The property to be searched consists of:

AT&T Cingular Flex EA211101 cell phone; IMEI 353786872430704

The **Subject Electronic Device** is in the custody of the FBI Binghamton Resident Agency, 15 Henry Street, #321, Binghamton NY 13901.

ATTACHMENT B

Items to Be Seized

Items and information that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) & (a)(5)(B) (Receipt and Possession of Child Pornography), 2422(b) (attempted enticement of a minor), 2251(a)(sexual exploitation of a minor), 2250(a) (failure to register an e-mail address as required by SORNA), and 1470 (transferring obscene material to a minor):

a. Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

b. Internet history, including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

c. Chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

d. Correspondence or other documentation identifying persons transmitting through interstate or foreign commerce, including by mail or computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

f. Correspondence and other matter pertaining to the receipt and possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256,

and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

g. Child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.

h. Records showing the use or ownership of Internet accounts, including evidence of Internet usernames, screen names, or other Internet user identification.

i. Computer-related documentation that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

j. Any passwords, codes, or digital keys that provide access to any computer hardware, computer software, computer-related documentation, or electronic data records.

k. Documents and records regarding the ownership and/or possession of electronic media being searched.

This authorization includes all electronic data that falls within the above categories, including deleted data, remnant data, and slack space.